# Social Engineering

*Por Samuel Hernández*

# What is Social Engineering?

- A hacker is known as a computer-knowledgeable person who is dedicated to detecting security flaws in computer systems.
- In the case of social engineering, it is the practice of obtaining confidential information through the manipulation of legitimate users, a social hacker.
- It does not require any kind of degree or diploma, simply enough malice and a repertoire of social/cyber manipulation skills.

# A bit of history...

- Social Engineering is a practice that has always existed, wherever there is information, there are always people looking for some way to get it illegitimately.

- The term Social Engineering was first used in 1894 to describe the importance of addressing social problems within industries, and then in 1911 it was used to describe how users of machinery in companies should work them as if they were social relationships.

- Today the term this term is used in the world of computing to describe the manipulation of legitimate users of a computer system by attackers looking to harm the system or extract some kind of valuable information.

# A bit of history... (Continued)

- Throughout the era of computer science, social engineering has become very prevalent in cyberattacks, it is estimated that 1 in 3 cyberattacks contain some form of social engineering as part of its process.
- These statistics are absolutely alarming, as these numbers continue to rise because regardless of the security of a computer system, the user in charge of handling it can become the biggest vulnerability and therefore be able to compromise the security of the entire system.
- Many people have been able to take advantage of this sad reality and have achieved great attacks just by sounding convincingly and having the skills to complete the cyberattack. One of the most notable people in this department is known as Kevin Mitnick, which we will see below.

# Kevin Mitnick: The Artist of Deception

Hacking is exploiting security controls on a technical, physical or **human element**.
-Kevin Mitnick

# Kevin Mitnick

- Known as one of the most feared hackers, Kevin was a very important figure in the world of hacking, not only for his technical skills, but for his immense skill for social engineering.
- Kevin started this kind of activity from the age of 12, when he used his "talents" so as not to have to pay a bus fare in Los Angeles, accomplished this by convincing the driver by pretending he didn't know that his card didn't have money or that he had to be on the bus for a school project.
- After that, he was persecuted and imprisoned for continuing to use his manipulation skills alongside techniques to gain access to companies and government agencies.

# Summary until now

- Social engineering is the practice of obtaining confidential information through the manipulation of legitimate users.
- It has been a term used with various definitions but is currently used to describe the process of social manipulation in the world of computing.
- Social engineering has become very prevalent in cyberattacks, it is estimated that 1 in 3 cyberattacks contain some form of social engineering as part of its process.

# How is it done?

- As mentioned above, the possibilities of the effect of a social engineering attack are endless, however, it doesn't always have to be on a large scale.
- I'm sure every one of us here is attacked with some kind of social engineering, even if we don't realize it or pay close attention to it.
- Next I will demonstrate several methods that attackers use to carry out these attacks, and analyze several real cases in which we can be exposed.

# Phishing

- It is one of the most common methods of attacks, as it is the simplest and most dangerous. It is known as "phishing" as it carries out an activity similar to fishing.
- It is about tricking a victim into voluntarily providing some kind of credential information that can be valuable to the attacker (passwords, credit cards, etc.).
- Victims receive an email or text message that a trusted person or organization, such as a co-worker, bank, or government office.
- Within these messages are some kind of warning or news that requires "immediate action", and usually takes them to a website that seems legitimate where users enter their data without knowing that it is false, and when they submit them, the attackers acquire the information which leads to other attacks (identity theft, money, etc.).

# Tipos de Phishing

- Spear Phishing
- Phishing
- Cloning
- 419/Nigerian Phone Phishing Scams

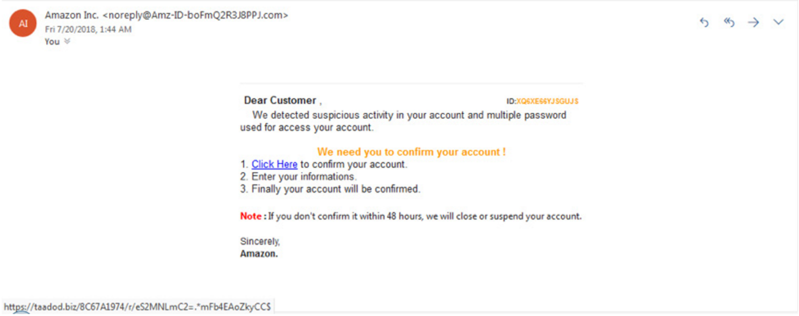
# How to identify it?

- It is extremely that when opening the email, recognize who sends it. If the email or phone number does not appear recognized, or claims to be from a company you know but the email is not familiar, it can be a phishing attack.
- Also, these emails usually contain alarming messages to try to induce some kind of immediate action through fear. This may be another sign.
- The message contains strange attachments or some kind of URL that is unreliable.

# Case Study #1

TV judge Shark Tank Barbara Corcoran was tricked into a nearly $400,000 social engineering and phishing scam in 2020. A cybercriminal was able to disguise himself as her assistant and sent an email to the accountant requesting a renewal payment related to real estate investments. He used an email address similar to legitimate ones. The fraud was only discovered after the accountant sent an email to the correct address of the assistant asking about the transaction.

# Examples



Amazon Inc. <noreply@Amz-ID-boFmQ2R3J8PPJ.com>
Fri 7/20/2018, 1:44 AM
You

Dear Customer , ID:XQ6XE66YJSGUJS

We detected suspicious activity in your account and multiple password used for access your account.

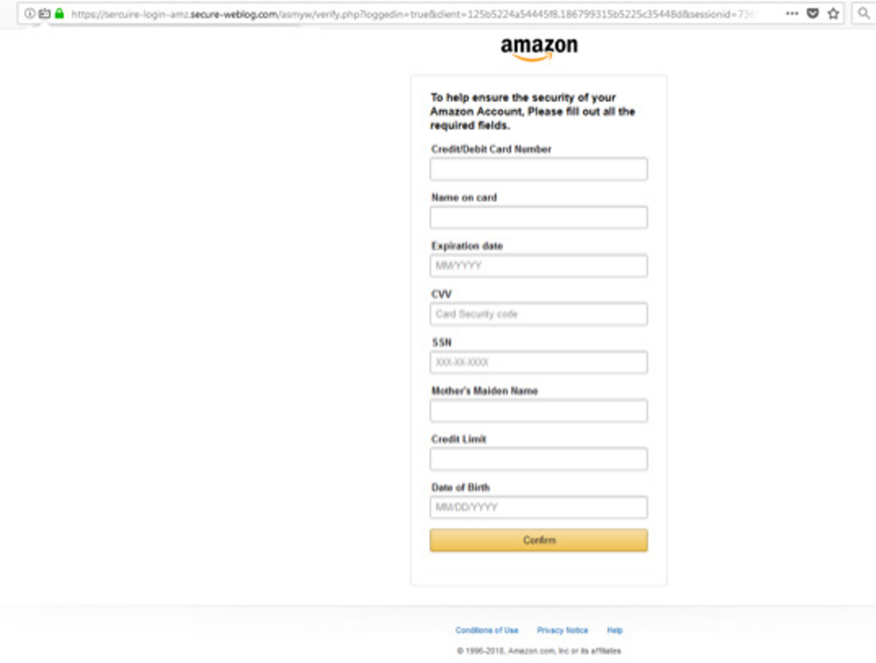
**We need you to confirm your account !**

1. Click Here to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.

**Note :** If you don't confirm it within 48 hours, we will close or suspend your account.

Sincerely,
**Amazon.**

https://taadod.biz/8C67A1974/r/eS2MNLmC2=.*mFb4EAoZkyCC$



https://sercuire-login-amz.secure-weblog.com/asmyw/verify.php?loggedin=true&client=125b5224a54445f8.186799315b5225c35448d&sessionid=73

**To help ensure the security of your Amazon Account, Please fill out all the required fields.**

Credit/Debit Card Number

Name on card

Expiration date: MM/YYYY

CVV: Card Security code

SSN: XXX-XX-XXXX

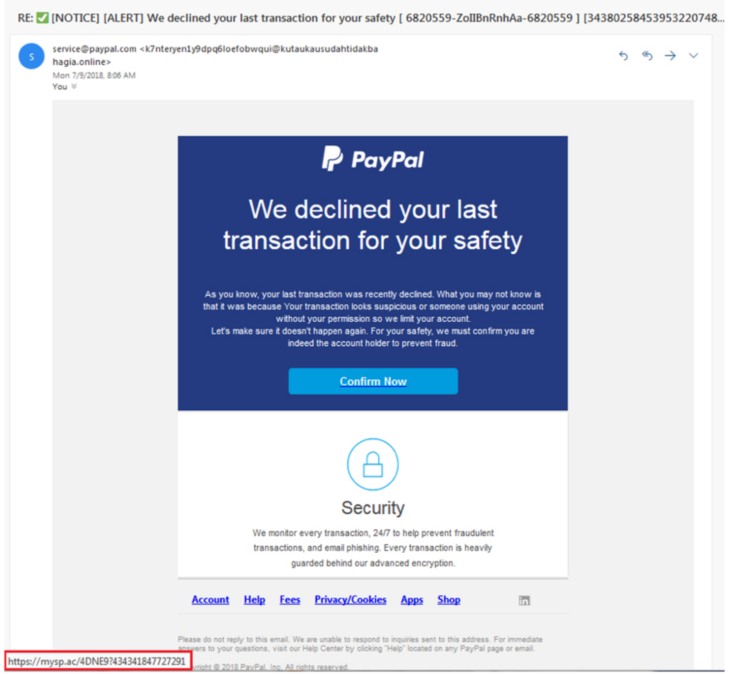
Mother's Maiden Name

Credit Limit

Date of Birth: MM/DD/YYYY

© 1996-2018, Amazon.com, Inc or its affiliates

# Examples



RE: ✅ [NOTICE] [ALERT] We declined your last transaction for your safety [ 6820559-ZoIIBnRnhAa-6820559 ] [343802584539532207448...

service@paypal.com <k7nteryen1y9dpq6loefobwqui@kutaukausudahtidakba
hagia.online>
Mon 7/9/2018, 8:06 AM
You

PayPal

We declined your last transaction for your safety

As you know, your last transaction was recently declined. What you may not know is that it was because Your transaction looks suspicious or someone using your account without your permission so we limit your account.
Let's make sure it doesn't happen again. For your safety, we must confirm you are indeed the account holder to prevent fraud.

Security

We monitor every transaction, 24/7 to help prevent fraudulent transactions, and email phishing. Every transaction is heavily guarded behind our advanced encryption.

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

https://mysp.ac/4DNE9?434341847727291

yright © 2018 PayPal, Inc. All rights reserved.

# How to prevent it?

- Do not open emails/texts other than recognized senders.
- Pass the cursor over the link to know where you're going without pressing it.
- Do not click on links without knowing exactly where they take you.
- Never open or download attachments if you are not sure where they come from.
- Find the website's digital certificates (SSL/HTTPS).

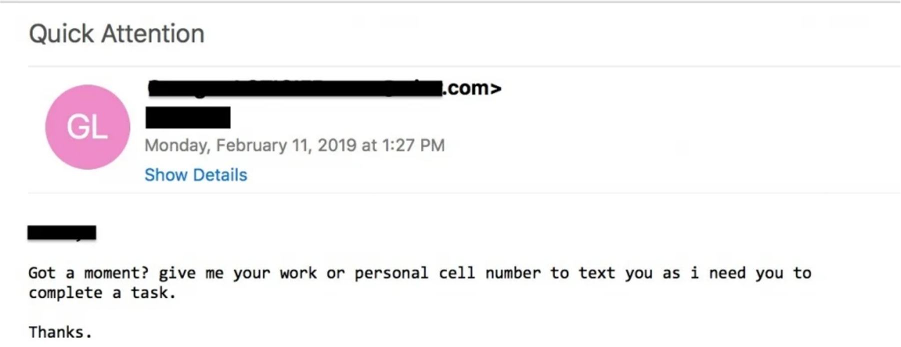
# Pretexting

- Another type of phishing, pretexting is more tied to phone calls, although it can also occur via email.
- With these calls, the attacker seeks to extract information that can lead to a continuation with another attack.
- It is known as pretexting as attackers seek a pretext or a situation built to put the victim in a vulnerable situation.
- Unlike phishing, pretexting seeks to create a sense of trust and security with the victim

# How to identify it?

- The calls are from an unknown number.
- Calls have the number blocked (or a Spam Risk alert appears)
- Senders are made to pass for known or trusted people asking for some kind of help or are offering some kind of reward or money, help with credit and even possible job offers.

# Examples



Quick Attention

GL

[redacted].com>

[redacted]

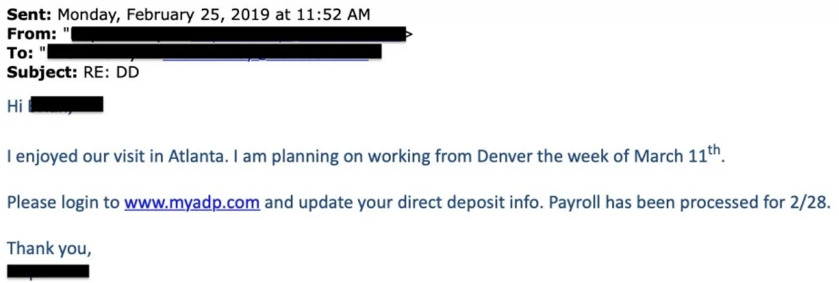
Monday, February 11, 2019 at 1:27 PM

Show Details

[redacted]

```
Got a moment? give me your work or personal cell number to text you as i need you to
complete a task.

Thanks.
```



**Sent:** Monday, February 25, 2019 at 11:52 AM
**From:** "[redacted]>
**To:** "[redacted]
**Subject:** RE: DD

Hi [redacted]

I enjoyed our visit in Atlanta. I am planning on working from Denver the week of March 11th.

Please login to www.myadp.com and update your direct deposit info. Payroll has been processed for 2/28.

Thank you,
[redacted]

# Case Study #2

Due to a social engineering scam, BEC, Cabarrus County in the United States suffered a loss of $1.7 million in 2018. Using malicious emails, the hackers switched to county providers and requested payments from a new bank account. According to the investigation, after the money was transferred, it was diverted to several accounts. In the emails, the scammers submitted seemingly legitimate documentation.

# How to prevent it?

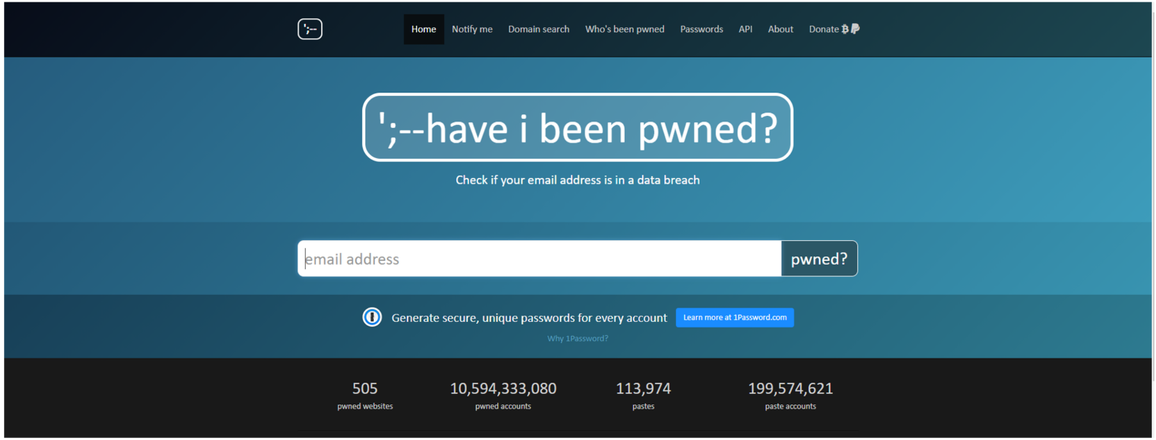
- Make sure that the numbers are recognized (and in the case of emails as well).
- Use identification tips to determine if it's an attack.
- Never access any help/reward that is offered as it is a manipulation tactic.
- Stay on top of your game by following the scamming trends, news, etc.

# Other types of social engineering attacks

- Dumpster Diving
- Physical Access Attacks
- Ransomware
- Baiting

# Interactive exercise

- In the next exercise, we will enter a website that aims to detect if any email or password you use has been found within a data breach. This will help you find out if your credentials and accounts may be at risk right now.
- URL: https://haveibeenpwned.com/



';--have i been pwned?

Check if your email address is in a data breach

email address

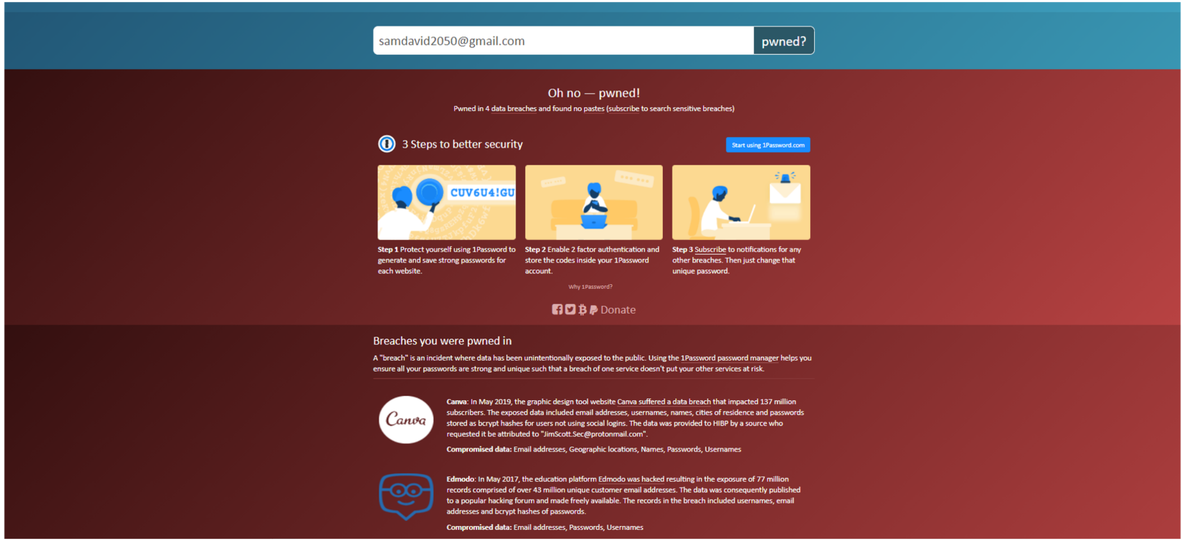
Generate secure, unique passwords for every account

505 pwned websites

10,594,333,080 pwned accounts

113,974 pastes

199,574,621 paste accounts



samdavid2050@gmail.com

Oh no — pwned!

Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.

**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.

**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**Canva**: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Email addresses, Geographic locations, Names, Passwords, Usernames

**Edmodo**: In May 2017, the education platform Edmodo was hacked resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords.

**Compromised data:** Email addresses, Passwords, Usernames

# Important precautions

- Ensure that your computer or system's antivirus/antimalware is installed appropriately.
- Recommend that the administrator implement some form of anti-phishing software that identifies the possibility of suspicious email or other suspicious activity. Do not open emails/texts other than recognized senders.
- Never open or download attachments if you are not sure where they come from.
- Use Two Factor Authentication.
- Change passwords every three months. He was judicious, not curious.

# Thank you so much for your attention! It's been a pleasure.

Any questions or doubts?